

QUADRATIC RESIDUES AND A NEW INFINITY OF ORDERS FOR WHICH A CONJECTURE OF RYSER ABOUT CIRCULANT HADAMARD MATRICES HOLDS

LUIS H. GALLARDO

ABSTRACT. For every positive integer k such that $k > 1$, there are an infinity of odd integers h with $\omega(h) = k$ distinct prime divisors such that there do not exist a Circulant Hadamard matrix H of order $n = 4h^2$. Moreover, our main result implies that for all of the odd numbers h , with $1 < h < 10^{13}$ there is no Circulant Hadamard matrix of order $n = 4h^2$.

1. INTRODUCTION

A complex matrix H of order n is *complex Hadamard* if $HH^* = nI$, where I_n is the identity matrix of order n , and if every entry of H/\sqrt{n} is in the complex unit circle. Here, the $*$ means transpose and conjugate. When such H has real entries, so that H is a $\{-1, 1\}$ -matrix, H is called *Hadamard*. If H is Hadamard and circulant, say $H = \text{circ}(h_1, \dots, h_n)$, that means that the i -th row H_i of H is given by $H_i = [h_{1-i+1}, \dots, h_{n-i+1}]$, the subscripts being taken modulo n , for example $H_2 = [h_n, h_1, h_2, \dots, h_{n-1}]$. A long standing conjecture of Ryser (see [12, pp. 134]) is:

Conjecture 1.1. *Let $n \geq 4$. If H is a circulant Hadamard matrix of order n , then $n = 4$.*

Details about previous results on the conjecture and a short sample of recent related papers are in [13], [11], [2] [3], [5], [4], [8] and the bibliography therein, [9].

The object of the present paper is to substantially extend the range of known n 's for which Ryser's Conjecture holds.

Our main result is:

Theorem 1.2. *For every positive integer k such that $k > 1$, there are an infinity of odd integers h with $\omega(h) = k$ distinct prime divisors such that there do not exist a circulant Hadamard matrix H of order $n = 4h^2$.*

Our result is a simple consequence (see Lemma 2.5) of a deep result of Arasu (see [1, Theorem 4, part (i)] and Lemma 2.2 below). By using the Hadamard-Barker's data in the web site of M. Mossinghoff (see [10]) and our main key Lemma 2.5 below, we are also able to prove (by computer computations) the following new result.

Proposition 1.3. *Let S be the set of all integers $n = 4h^2$ with odd h such that $1 < h < 10^{13}$. For all $s \in S$ there is no circulant Hadamard matrices of order n .*

Date: November 11, 2014.

2010 Mathematics Subject Classification. Primary 11A07; Secondary 15A24, 15B34.

Key words and phrases. Quadratic residues, Weighing matrices, Circulant Hadamard matrices, Ryser's Conjecture.

These results implies corresponding results for the existence of Barker sequences (see section 4). Of course, by using Lemma 2.5 combined with results obtained by other methods it is possible to improve our numerical results herein. For example, by applying the lemma to already known h 's satisfying $h < 10^{24}$ (see some of them in the web site already cited) and for which all other methods have failed, etc. Two more examples: (a) In about 6 seconds computation in an old computer our Lemma 2.5 eliminated the only possible obstruction known for h , namely $h = 31540455528264605$ in order that a Barker sequence exist with $13 < 4h^2 < 10^{33}$, (see [3, Theorem 1]). (b) In about 3 seconds the first 6 values of h in between $10^{16.5}$ and $5 \cdot 10^{24}$

[66687671978077825, 866939735715011725, 1293740836374709805,

6468704181873549025, 16818630872871227465, 84093154364356137325];

(over 18) in [3, Table 2] were also eliminated as before. However, it is easy to see that there are values of h that satisfy all the assumptions of Lemma 2.5, besides the assumption on the possible existence of H . Indeed some experiments with small values of h , say $h \leq 10000$, suggest that, at least for these values, there exist about 5/100 of h 's for which all the orders appearing in the lemma are odd.

2. SOME TOOLS

First of all we recall the notion of a weighing matrix.

Definition 2.1. Let n be a positive integer. Let k be a positive integer. A *weighing matrix* W of order n and weight k is an $n \times n$ matrix W with all its entries belonging to the set $\{-1, 0, 1\}$ such that

$$WW^T = kI_n$$

where the " T " means "transpose" and I_n is the identity matrix of order n .

We recall the result of Arasu ([1, Part (i) of Theorem 4]).

Lemma 2.2. Let n, k be positive integers such that $n = p^a \cdot m$, $k = p^{2b} \cdot u^2$, where a, b, m, u are positive integers such that the prime number p does not divide m and p does not divide u . Assume that there exists an integer t such that

$$p^t \equiv -1 \pmod{m}.$$

If there exists a weighing matrix W of order n and of weight k that is circulant then $p = 2$ and $b = 1$.

We use the obvious decomposition below of a circulant Hadamard matrix of even order n in four blocks of order $n/2$, (see [9] for another result based on the same decomposition), in order to build a weighing matrix attached to H .

Lemma 2.3. Let $H = \text{circ}(h_1, \dots, h_n)$ be a circulant Hadamard matrix of order n . Then

(a)

$$H = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

where A, B are matrices of order $\frac{n}{2}$.

(b) $K = A + B$ is circulant with entries in $\{-2, 0, 2\}$.

We build now the weighing matrix.

Lemma 2.4. *Let h be an odd positive integer. Assume that H is a circulant Hadamard matrix of order n , where $n = 4h^2$. Then, there exists a weighing matrix C of order $n/2$ and weight $n/4$.*

Proof. Set $C = \frac{A+B}{2}$ where A and B are defined by Lemma 2.3. One has then that C is circulant, of order $n/2 = 2h^2$ with all its entries in $\{-1, 0, 1\}$. From $HH^* = I_n$, one gets by block multiplication $AA^* + BB^* = nI_{n/2}$ and $AB^* + BA^* = 0$. Thus,

$$(1) \quad 4 \cdot CC^* = AA^* + AB^* + BA^* + BB^* = AA^* + BB^* = nI_{n/2}.$$

It follows from (1) that C is a weighing circulant matrix of order $n/2$ and weight $n/4$. \square

We are now ready to show our main result from which, (essentially), we will be obtaining all our results.

Lemma 2.5. *Let h be an odd positive integer exceeding 1. Assume that H is a circulant Hadamard matrix of order n , where $n = 4h^2$. Let p be a prime divisor of h and r be the positive integer such that $p^r \mid h$ but $p^{r+1} \nmid h$. Set $s = h/p^r$. Let $o_m(p)$ be the order of p in the multiplicative group $G = (\mathbb{Z}/m\mathbb{Z})^*$ of invertible elements of the ring $\mathbb{Z}/m\mathbb{Z}$, where $m = 2s^2$. Then,*

$$o_m(p)$$

is an odd number.

Proof. Assume, to the contrary, that $o_{2s^2}(p)$ is even, say $o_{2s^2}(p) = 2f$. Then $p^f \equiv -1 \pmod{2s^2}$. Then, by Lemma 2.2 applied to the weighing matrix C , of order $n/2$ and weight $n/4$, defined by Lemma 2.4 with $a = 2r$, $b = r$, $m = 2s^2$, and $u = s$ that are all positive integers, and observing that we have $\gcd(p, m) = 1$ and $\gcd(p, u) = 1$, we obtain the contradiction

$$(2) \quad p = 2.$$

This proves the lemma. \square

Remark 2.6. Of course, if in the proof of Lemma 2.5, we apply Lemma 2.2 to the full circulant weighing matrix H (of order n , and of weight n), instead to applying it to C , we obtain no contradictions.

In order to complete the results the following simple arithmetic result is key.

Lemma 2.7. *Let p and q be two odd prime numbers such that the orders $o_q(p)$, the order of p modulo q , and $o_p(q)$, the order of q modulo p , are both odd. Then*

$$\left(\frac{p}{q}\right) = 1 \quad \text{and} \quad \left(\frac{q}{p}\right) = 1.$$

where (\cdot) is the Legendre's symbol.

Proof. Since $d := o_q(p)$ is odd, we have $p \equiv \left((1/p)^{\frac{d-1}{2}}\right)^2 \pmod{q}$. Analogously $e := o_p(q)$ odd implies $q \equiv \left((1/q)^{\frac{e-1}{2}}\right)^2 \pmod{p}$. The result follows. \square

3. PROOF OF THEOREM 1.2 AND OF PROPOSITION 1.3

3.1. Proof of Theorem 1.2. Assume that there are only a finite number of such odd integers h . Then, by Lemma 2.5, there exists some odd positive integer h_0 such that for any odd integer h with $h \geq h_0$ every prime number p such that $p \mid h$, say, $h = p^r \cdot s$, with $p^{r+1} \nmid h$, satisfy

$$(3) \quad o_{2s^2}(p) \text{ is odd.}$$

Thus, (3) implies that for every odd prime divisor q of $2s^2$ one has

$$(4) \quad o_q(p) \text{ is odd.}$$

Write now $h = q^t d$ with $q \nmid d$. one has also,

$$(5) \quad o_{2d^2}(q) \text{ is odd.}$$

Thus, for every odd prime divisor r of $2d^2$ one has

$$(6) \quad o_r(q) \text{ is odd.}$$

Choose $r = p$ in (6). One gets

$$(7) \quad o_p(q) \text{ is odd.}$$

This implies, by Lemma 2.7 that $\left(\frac{p}{q}\right) = 1$ and that $\left(\frac{q}{p}\right) = 1$ for any other prime factor q of h . But this is false, since we can always choose two distinct primes p_1 and p_2 both larger than h_0 and with, e.g.,

$$\left(\frac{p_1}{p_2}\right) = 1 \quad \text{and} \quad \left(\frac{p_2}{p_1}\right) = -1,$$

and take

$$h = p_1 \cdot p_2 \cdots p_k$$

with any other distinct prime numbers (when $k > 2$), p_2, \dots, p_k . This proves the theorem.

3.2. Proof of Proposition 1.3. It is known (see [3]) that for all elements of S but for a subset T containing 1371 elements h the result holds. Using Lemma 2.5 and a straightforward (included below for completeness) computer program that checked the conclusion of the above lemma for all these h 's, and after about 7 minutes of computation, we obtained the result.

Here the program used:

```
# n's 4*h**2, with constraints on its odd prime divisors
```

```
with(numtheory):
```

```
tesp := proc(h)
local p,m,par,pris,el,mo,rr;
pris := ifactors(h); pris := op(2,pris);
if nops(pris) = 1 then RETURN(0); fi;
for par in pris do
p := op(1,par); m := op(2,par); el := iquo(h,p**m); mo := 2*el**2;
rr := order(p,mo);
if modp(rr,2) = 0 then RETURN(0); fi;
od;
RETURN(1);
end;
```

```

# checks the 1371 elements of the list uvals

seelm := proc()
local p,lis,c,st;
st := time(); c := 0; lis := [];
read(mike1):
for p in uvals do
if tesp(p) = 1 then print([c,[1371],p]); lis := [p,op(lis)]; fi;
c := c+1;
if modp(c,100) = 0 then print([time() -st,c]) fi;
od;
lis;
end;

# the actual program runned is:

interface(prettyprint=0):
interface(quiet=true): st := time(); time() -st;
st := time(); z := seelm(); time() -st;

quit;

```

4. BARKER SEQUENCES

Suppose x_1, x_2, \dots, x_n is a sequence of 1 and -1 . We recall the following definition.

Definition 4.1. A sequence c_1, c_2, \dots, c_{n-1} , where

$$c_j = \sum_{i=1}^{n-j} x_i \cdot x_{i+j}$$

and the subscripts are defined modulo n , is called a *Barker* sequence of length n provided $c_j \in \{-1, 0, 1\}$, for all $j = 1, 2, \dots, n-1$.

The main known result is the following, (see [13], [7]).

Lemma 4.2. *If there exists a Barker sequence of length $n > 13$ then there exists a circulant Hadamard matrix of order n .*

Corollary 4.3. *For an infinity of odd integers h 's with an arbitrary fixed number k of distinct prime divisors there do not exists a Barker sequence of length $4h^2 > 13$. Moreover, there do not exists a Barker sequence of length $4h^2 > 13$ for all odd integers h such that $1 < h < 10^{13}$.*

Proof. Follows from Lemma 4.2, from Theorem 1.2 and from Proposition 1.3. \square

ACKNOWLEDGEMENTS

We are indebted to Michael J. Mossinghoff for sending us a special file, ready for computations, containing all odd integers h less than 10^{13} (used in the proof of Proposition 1.3, above) for which all previous known results, cannot decide whether or not for $n = 4h^2$ there exist a circulant Hadamard matrix of order n . Thanks also to Carlos M. da Fonseca for patience and to the anonymous referees of a related paper of mine, containing a too optimistic result, for inspiration to build the present paper.

REFERENCES

- [1] K. T. Arasu, *A reduction theorem for circulant weighing matrices*, Australas. J. Combin. **18** (1998), p. 111–114.
- [2] P. Borwein, M. J. Mossinghoff, *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. **53**(3) (2009), p. 149–163.
- [3] P. Borwein, M. J. Mossinghoff, *Wieferich pairs and Barker sequences, II*, LMS J. Comput. Math. **17** (1) (2014), 24–32.
- [4] R. A. Brualdi, *A note on multipliers of difference sets*, J. Res. Nat. Bur. Standards Sect. B **69** (1965), p. 87–89.
- [5] R. Craigen, G. Faucher, R. Low, T. Wares, *Circulant partial Hadamard matrices*, Lin. Alg. Appl. **439**, 3307–3317, 2013.
- [6] P. J. Davis, *Circulant matrices*, 2nd ed., New York, NY: AMS Chelsea Publishing, xix, 250 p. (1994).
- [7] S. Eliahou, M. Kervaire, *Corrigendum to: “Barker sequences and difference sets”* [Enseign. Math. (2) 38, no. 3–4, 345–382, 1992], Enseign. Math. (2) 40, no. 1–2, 109–111, 1994.
- [8] R. Euler, L. H. Gallardo, O. Rahavandrainy, *Sufficient conditions for a conjecture of Ryser about Hadamard Circulant matrices*, Lin. Alg. Appl. **437**, 2877–2886, 2012.
- [9] L. Gallardo, *On a special case of a conjecture of Ryser about Hadamard circulant matrices*, Appl. Math. E-Notes **12**, 182–188, 2012.
- [10] M. J. Mossinghoff, “Wieferich prime pairs, Barker sequences, and circulant Hadamard matrices”, 2013, <http://www.cecm.sfu.ca/mjm/WieferichBarker/>.
- [11] K. H. Leung, B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Designs, Codes and Cryptography **64**, 143–151, 2012.
- [12] H. J. Ryser, *Combinatorial mathematics*. The Carus Mathematical Monographs, No. 14 Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York 1963 xiv+154 pp.
- [13] J. Storer, R. Turyn, *On binary sequences*, Proc. Am. Math. Soc. **12** (1961), p. 394–399.
- [14] S. LANG, *Algebra*. 3rd revised ed. Graduate Texts in Mathematics 211, New York, NY: Springer, xv, 914 p. (2002).

UNIVERSITY OF BREST, MATHEMATICS, 6, AV. LE GORGEU, C.S. 93837, 29238 BREST CEDEX 3, FRANCE.

E-mail address: Luis.Gallardo@univ-brest.fr